IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEBRASKA

UNITED STATES OF AMERICA	:	
	:	
	:	
v.	:	**Case No. 13-cr-108**
	:	
	:	
DAVID SMITH	:	

BRIEF IN SUPPORT OF MOTION TO SUPPRESS EVIDENCE RESULTING FROM SEARCH OF ACTIVIATING COMPUTER IP ADDRESS 24.154.177.245

Factual Background:

On or about November 15, 2012, federal agents seized three computer servers at Power DNN/Perigon and Cosentry, in Bellevue, Nebraska. Forensic examination of one server confirmed that it was hosting a child pornography bulletin board (CPBB), one of which was known as "Hidden Service B." These websites were on the Tor-Network or "onion router", a network that creates anonymity for the user, allowing them to access websites that can be set up as "hidden services", such as "Hidden Service B". A user can only access the "hidden services" if he/she is operating in the Tor-network and obtains the algorithm-based web address from other users of the board or from internet postings describing the location and content of the hidden service.

Upon seizure of the servers, law enforcement decided to take over and operate "Hidden Service B"[1] in an effort to identify the users of the website through their IP address. The computer server hosting "Hidden Service B" was taken to a Government facility and controlled and operated by federal agents from November 18, 2012 until December 2, 2012. Attachment A of the Warrant listed the "Place to be Searched" as use of a network investigative technique (NIT) to be deployed on the computer server operating the Tor-Network child pornography bulletin board "Hidden Service B" URL s7cgvirt5wvojli5.onion, located on a computer server at a government facility in the District of Nebraska, obtaining information from activating computers, the users of which access any page of this website.[2] Attachment B of the Warrant listed the "Information to be Seized" as the activating computer's actual IP address and date/time the NIT determines what that IP address is, the unique session identifier sent by "Hidden Service B", and the type of operating system running on the computer, including type, version and architecture.[3]

The NIT was characterized as a seizure of an electronic communication or electronic information under 18 U.S.C. § 3103a(b)(2), deemed necessary to secure certain registry-

[1] "Hidden Service B" was a name given to the website by law enforcement and later presented as "Website A" to the federal grand jury and the Application for Search Warrant for the Defendant's residence.
[2] Attachment A lists several sections of "Hidden Service B" that have been identified as child pornography.

type information that would assist in identifying the computer, its location, and the user of the computer accessing "Hidden Service B", due to the method by which the Tor-Network protects the anonymity of its users. The Search Warrant sought, pursuant to F.R.C.P. 41(f)(3) and 18 U.S.C. §§ 3103a(b)(1) and (3), to delay notice up to 30 days of the execution of the search warrant, as notice of the use of the NIT would risk destruction of or tampering with evidence, such as files stored on the computers of individuals accessing "Hidden Service B". The Search Warrant Affidavit averred that the investigation had not yet identified individuals whom notice can be given, and that sufficient time would be required to identify individuals after the NIT was deployed and extracted information included in Attachment B. See ¶ 24.

On November 27, 2012, the NIT search of an activating computer revealed that IP Address 24.154.177.245 accessed website "Hidden Services B" from 4:32 a.m. to 4:38 a.m. Sometime between November 27, 2012 and March 20, 2013, IP Address 24.154.177.245, through the use of an administrative subpoena, was determined to belong to an Armstrong Cable Services subscriber named James Smith living at 114 Brown Avenue, Butler, Pennsylvania.

---

[3] Attachment B limited the information seized to violations of 18 U.S.C. §§ 2252A(g); 2251(d)(1),(e); 2252A(a)(2)(A),(b)(1); and/or 2252A(a)(5)(B).

On March 20, 2013, a federal grand jury sitting in the District of Nebraska returned a 2 Count Indictment charging John Doe #2 a/k/a user of IP Address 24.154.177.245[4] on November 27, 2012 with knowingly receiving and attempting to receive child pornography, as defined in Title 18 U.S.C. § 2256(8)(A), in violation of Title 18, U.S.C., §§ 2252A(a)(2) and (b)(1); and with knowingly accessing with intent to view a computer disc and other material that contained an image of child pornography, as defined in Title 18 U.S.C. § 2256(8)(A) in violation of Title 18, U.S.C., § 2252A(a)(5)(B).

On April 11, 2013, a Search Warrant was executed at the Smith residence at 114 Brown Avenue, Butler, Pennsylvania. The Affidavit, in part, stated that that "a user of the Internet account at 114 Brown Avenue . . . has been linked to "Website A", a/k/a "Hidden Service B", a website whose primary purpose is to advertise and distribute child pornography." Specifically IP 24.154.177.245 accessed a page described as "Male Jail Bait" and message thread number 1503 "Gun Boy", which had been posted on "Website A" on November 22, 2012 while under Government control. That thread message contained images of child pornography.

On May 15, 2013, Agent Tarpinian submitted a request and search warrant from the Western District of Pennsylvania

[4] John Doe #2 was identified as David Smith in the Second Superseding Indictment

to the FBI Digital Analysis and Research Center (DARC) authorizing the search of "specimens" or electronic communication devices, including desktop computers, laptop computers, and hard drives that were seized from 114 Brown Avenue, Butler, PA on April 11, 2013. A Report of Examination by DARC relating to IP address 24.154.177.245, dated October 7, 2013, detailed findings of various images of suspected child pornography on specimens QHQ011, QHQ018 and QHQ029.

On October 23, 2013, a federal grand jury sitting in the District of Nebraska returned a 2 Count Indictment charging David Smith a/k/a user of IP Address 24.154.177.245 on November 27, 2012 with knowingly receiving and attempting to receive child pornography, as defined in Title 18 U.S.C. § 2256(8)(A), in violation of Title 18, U.S.C., §§ 2252A(a)(2) and (b)(1); and with knowingly accessing with intent to view a computer disc and other material that contained an image of child pornography, as defined in Title 18 U.S.C. § 2256(8)(A) in violation of Title 18, U.S.C., § 2252A(a)(5)(B). The Defendant was arrested on November 15, 2013 by FBI agents based on its investigation of Website A, and the warrant issued as a result of this Indictment.

Argument:

Rule 41(e)(2)(A)&(B) provides for the requirements of a Warrant Seeking Electronically Stored Information. The time for executing the warrant refers to the seizure or on-site copying of the media or information.

Rule 41(f)(1)(C) provides that the officer executing the warrant must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken or leave a copy of the warrant and receipt at the place where the officer took the property.

Rule 41(f)(1)(D) provides, in part, that the officer executing the warrant must promptly return it—together with a copy of the inventory—to the magistrate judge designated on the warrant. The officer may do so by reliable electronic means.

Rule 41(f)(3) provides, in part, that upon the government's request, a magistrate judge may delay any notice required by this rule if the delay is authorized by statute.

Title 18, United States Code, § 3103a(b) Delay.-With respect to the issuance of any warrant or court order under this section, or any other rule of law, to search for and seize any property or material that constitutes evidence of

a criminal offense in violation of the laws of the United States, any notice required, or that may be required, to be given may be delayed if-

(1) the court finds reasonable cause to believe that providing immediate notification of the execution of the warrant may have an adverse result (as defined in section 2705, except if the adverse results consist only of unduly delaying a trial);

(2) the warrant prohibits the seizure of any tangible property, any wire or electronic communication (as defined in section 2510), or, except as expressly provided in chapter 121, any stored wire or electronic information, except where the court finds reasonable necessity for the seizure; and

(3) the warrant provides for the giving of such notice within a reasonable period not to exceed 30 days after the date of its execution, or on a later date certain if the facts of the case justify a longer period of delay.

Title 18, United States Code, § 3103a(c) Extensions of delay.-any period of delay authorized by this section may be extended by the court for good cause shown, subject to the condition that extensions should only be granted upon an updated showing of the need for further delay and that each additional delay should be limited to periods of 90 days or

less, unless the facts of the case justify a longer period of delay.

A. The Government failed to provide notice pursuant to Rule 41 and 18 U.S.C. § 3103a

The Application for a Search Warrant "In the Matter of the Search of computers that access the website "Hidden Service B" located at s7cgvirt5wvojli5.onion" did request delayed notice of 30 days under 18 U.S.C. § 3103a. The issuing magistrate judge in this case did find on the Search and Seizure Warrant that *immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property will be searched or seized – for 30 days (not to exceed 30).* (emphasis added).

The NIT search of the activating computer, IP address 24.154.177.245, occurred on November 27, 2012. § 3103a(b)(3) dictates that notice, i.e. a copy of the warrant and a receipt for the property taken, must be provided within a reasonable period not to exceed 30 days after the date of its execution **to the person from whom, or from whose premises, the property was taken** (emphasis added). See *Rule 41(f)(1)(C).* The person from whom, or from whose premises, the property was taken was James Smith. Mr. Smith is the deeded owner of 114 Brown Avenue, Butler, Pennsylvania and,

according to the ISP, Armstrong Cable Services, was the internet subscriber at this address. James Smith was not provided notice of the NIT search and seizure. A copy of the administrative subpoena issued to Armstrong Cable Services has not been provided to Counsel for the Defendant as a part of the Rule 16 documents provided to date.

It is believed and therefore averred that the officer executing the NIT warrant, presumably Agent Tarpinian, made a return of the warrant to the magistrate judge on or about November 19, 2012, which was prior to reception of any activating computers on Website A, via employment of the NIT. If so, *Rule 41(f)(1)(D)* was also violated since it provides that the warrant must promptly be returned to the magistrate judge *together with a copy of the inventory*. If no NIT search had occurred as of the date of the warrant's return, than no inventory could have been provided to the court. A copy of the warrant return and inventory has not been provided to Counsel for the Defendant as a part of the Rule 16 documents provided to date.

The Government argues that notice is to be provided to the user of the activating computer and, in support of that, points to ¶ 30 of the Affidavit, which requested authorization pursuant to 18 U.S.C. § 3103a(b)(3), to satisfy the notice requirement of F.R.C.P. 41(f)(3):

> the Government may delay "providing a copy of the search warrant and the receipt for any property taken

> for thirty (30) days after a user of an activating computer that accessed 'Hidden Service B' has been identified to a sufficient degree as to provide notice, unless notification is further delayed by court order."

The Government's argument lacks merit for three reasons. One, the Search Warrant expressly authorizes and limits the officer executing this warrant to delay notice to the person who, or whose property will be searched or seized – for 30 days (not to exceed 30). The authorization does not provide for an open-ended delay, as requested in ¶ 30 of the Affidavit, "for thirty (30) days after a user of an activating computer that accessed 'Hidden Service B' has been identified to a sufficient degree as to provide notice". Two, had the Government desired a further extension of the notice requirement, which is allowed via Rule 41(f)(3) and 18 U.S.C. § 3103a(c) [any period of delay may be extended by the court for good cause shown], than proper application should have been made to the magistrate judge. Clearly it was not and, therefore, the 30 days expired on December 27, 2012. Third, as stated previously and notwithstanding the averments contained in ¶¶ 24 and 30 of the Affidavit in Support of the Application for the NIT Search Warrant, James Smith is the aggrieved party, not his son, David Smith. Since he is the property owner of the searched premises, 114 Brown Avenue, and IP subscriber then, pursuant to Rule 41(f)(1)(C), it is he who should be provided notice of the search and inventory of the property

or information seized. Assuming that James Smith was identified via his ISP in late November of 2012, just as Messrs. Cottom (11-26-2012) and Pittman (11-27-2012) were, then notification clearly could have been rendered within the 30 days as provided for in the Search and Seizure Warrant.

B. The Government's failure to provide notice was in reckless disregard of proper procedures

"'[N]oncompliance with Rule 41 does not automatically require exclusion of evidence in a federal prosecution. Instead, exclusion is required only if a defendant is prejudiced or if reckless disregard of proper procedure is evident.' *United States v. Spencer,* 439 F.3d 905, 913 (8th Cir.2006) (internal citations and quotation marks omitted)." *United States v. Mutschelknaus, 592 F.3d 826, 829-830 (8th Cir. 2010).*

The Government asserts that the request that notice be delayed for 30 days "after a user of an activating computer that accessed [Website A] [had] been identified to a sufficient degree as to provide notice" [¶¶ 24 and 30]. If the Court agrees with this premise, the Defendant submits that a violation of Rule 41 still exists. This is based on the fact that, to date, no notice was ever provided to David Smith of the deployment of a NIT search and seizure of

certain electronic information. Unlike, Messrs. Cottom (notice of NIT provided on April 9, 2013 at his Identity and Detention Hearing in U.S. District Court for the Western District of New York, following his arrest and the search of his residence) and Pittman (notice of NIT provided on April 9, 2013 at his Initial Appearance in U.S. District Court for the Western District of Texas, following his arrest and the search of his residence), the Defendant, David Smith was never provided notice by the Government of the NIT search and resulting seizure, despite the search of his residence on April 11, 2013 and Initial Appearance in U.S. District Court for the Western District of Pennsylvania, following his arrest on November 15, 2013. As such, even under the theory that delayed notice to the perpetrator (verses the property owner) conforms to the notice requirements provided for in Rule 41(f)(3) and 18 U.S.C. § 3103a(b), the argument fails because the Defendant was never given notice of NIT search and seizure of information, and never provided a receipt or inventory of the property or information taken.

The Government's failure to give notice of the NIT search and seizure was in reckless disregard of proper procedures in two ways. One, while the NIT search warrant affidavit disclosed the need and requested delay notice until after a person to whom notice could be given was identified, that "request" was not honored by the magistrate

judge, who expressly limited the Government to no more than 30 days to provide said notice. By ignoring this delay limitation imposed by the Court, federal agents acted in bad faith by circumventing federal requirements, specifically Rule 41, by unilaterally extending the delay period without court authorization, unlike *Mutschelknaus* (officers explicit request for an extension of time in their affidavit to perform an examination after the computer was seized, which was approved by the court, shows a manifest *regard* for the issuing judge's role in authorizing searches, rather than a 'bad faith [attempt] to circumvent federal requirements.'" *See United States v. Syphers,* 426 F.3d 461, 469 (1st Cir.2005)). *Id.*

Two, a more blatant violation of Rule 41 occurred by failing to provide David Smith with any notice of the NIT search and seizure. This failure goes well beyond any attempt to justify a delay, especially since the premise under 18 U.S.C. § 2705(2)(C), to wit, destruction of or tampering with evidence, was no longer an issue given the April 11, 2013 residential search and seizure, and the fact that one time co-defendants Cottom and Pittman were made aware of the use of the NIT search during the course of their respective residential searches and arrests in April 2013. This evidence and/or conduct of the agents

intentional and deliberate disregard of a provision in the Rule merits exclusion of the evidence obtained therein.

"We apply the exclusionary rule to violations of Rule 41 only if a defendant is prejudiced or reckless disregard of proper procedure is evident." *United States v. Bieri, 21 F.3d 811, 816 (8th Cir. 1994).*

The Government also asserts that the Defendant had no expectation of privacy because there was no actual entry into the residence and no seizure of property pursuant to the NIT authorization. A seizure of property triggering Fourth Amendment protection is "some meaningful interference with an individual's possessory interests in that property." *Dixon v. Lowery, 302 F.3d 857, 862 (8th Cir. 2002).* The electronic age has transformed the traditional concept of tangible property to include intellectual property and how that property is stored. The Government's assertion that the NIT "merely collected information" such as IP address and type of operating system is misplaced. The NIT, in essence, was a virus intentionally implanted in the Defendant's computer causing it to perform a function (provide various types of information) it would not have ordinarily performed. The same type of intrusion as an agent placing a tracking device on a vehicle forcing a surreptitious influx of information without the vehicle owner's knowledge or consent.

The expectation of privacy rests with the ability to be secure in ones persons, houses, papers and effects against unreasonable searches and seizures. The Government's intentional surreptitious intrusion into an individual's computer operating system or hard drive is in fact a search and, hence the forcible or surreptitious extraction of information in that computer equates to a seizure. If not why was a search warrant applied for in the first instance. Clearly Attachment B lists the property or information the Government sought to seize by way of the NIT search. To say now that there was no seizure as a result of the search is truly disingenuous.

C. Conclusion

The Defendant, David Smith, respectfully requests that this Honorable Court suppress all physical, electronic, documentary and testimonial evidence based upon the Government's failure to provide notice of the search and seizure of activating computer IP Address 24.154.177.245, and failure to provide an inventory of seized property/information within 30 days of November 27, 2012, pursuant to Rule 41 of the Federal Rules of Criminal Procedure and Title 18 U.S.C. § 3103a.

Respectfully submitted,

/s/ Stephen M. Misko
Stephen M. Misko, Esquire
Attorney for David Smith

CERTIFICATE OF SERVICE

I hereby certify that a true and correct copy of the foregoing **Brief in Support of Motion to Suppress Evidence Resulting from Search of Activating Computer IP Address 24.154.177.245** was served by ECF Electronic Mail, on the following parties, on this the 31st day of January, 2014:

Michael P. Norris, Esquire
United States Attorney's Office
Omaha, Nebraska
michael.norris@usdoj.gov

Keith A. Becker, Esquire
U.S. Department of Justice
Child Exploitation Section
Washington, D.C.
keith.becker@usdoj.gov

Sarah Chang, Esquire
U.S. Department of Justice
Child Exploitation Section
Washington, D.C.
sarah.chang@usdoj.gov

/s/ Stephen M. Misko
Stephen M. Misko, Esquire
Attorney for David Smith